DRAFT

Test Plan

For

Secure Biometrics
Match-on-Card (sBMOC)

Technical Feasibility Study

Prepared for:
National Institute of Standards and Technology

Please send comments to:
william.macgregor@nist.gov

May 2007

Table of Contents

1. PURPOSE

FIPS 201-1 and associated NIST Special Publications define a method to perform biometric authentication of a PIV cardholder when the PIV Card is inserted into a contact smart card reader. In some use cases, however, contactless (Radio Frequency) operation is required. Security of RF communication has been a hindrance to specifying biometric data transfer over the contactless interface. The transaction data can be secured through ISO/IEC 7816 secure messaging; however, this operation can be time intensive and may not meet real-world performance requirements. To determine technical feasibility with current smart card devices, NIST will conduct a performance study of secure Biometric Match-On-Card (sBMOC) using a secure protocol suitable to the contactless mode of operation. Ultimately, NIST may recommend an extension of PIV Card operation that achieves secure biometric authentication over contactless, however, production of a standard or draft standard is not an immediate goal of the study.

Secure BMOC can be used in place of, or with, PIN entry to achieve card activation. The study will build on PKI to create an authenticated, secure session similar to an SSL/TLS session between a web browser and a server. The approach never releases biometric data from the PIV Card; instead, it receives a sample template from a biometric reader, performs a match against an on-card reference template, and returns a Yes/No result to the reader.

A determination of technical feasibility requires baseline assumptions on the components used. We require that the smart card types tested be among those currently tested and validated through the NPIVP test program, modified only by firmware changes necessary to implement BMOC functionality. We do not require that the modified smart cards be validated through NPIVP or CMVP test programs for purposes of the feasibility study.

Currently, three manufacturers are known to provide BMOC firmware, and one of these has produced an algorithm validated by the Ongoing MINEX testing. Preliminary tests have shown that a BMOC operation for physical access could be performed in less than 500 milliseconds without secure messaging. Tests of PKI transaction times suggest that the approach could meet the performance criterion of less than 2.5 seconds per transaction.

Objectives

FIPS 201-1 permits biometric data to be released from a PIV Card only across the contact interface of the card, and only after activation of the card by presentation of the cardholder's PIN. These restrictions achieve two security objectives: communication of biometric data occurs only over a trusted communication channel that is not easily subject to eavesdropping attacks (namely, the wired contacts inside the smart card reader); and the PIV cardholder implicitly attests to the legitimacy of the smart card reader, as indicated by their entry of the PIN on the smart card reader keypad. FIPS 201-1 enables biometric authentication to occur without imposing a technical requirement for automatic authentication of smart card readers to PIV Cards, which was believed would add unacceptable key management costs. Note that a digital signature is on biometric data which can be used to authenticate originality. This feasibility study will evaluate the impact on transaction performance when the protocol observes the following security objectives:

- SO1: communication of biometric data shall occur only over a trusted channel that is not susceptible to eavesdropping attacks in the reader-to-card direction, nor spoofing or replay attacks in the card-to-reader direction; and

- SO2: communication of biometric data between the PIV Card and smart card reader shall occur only after the cardholder has indicated the reader is legitimate; and

- SO3: communication of biometric data from the PIV Card to the reader shall occur only after the cardholder has entered their PIN; and

- SO4: the approach should achieve the preceding security objectives without reader-to-smart-card authentication or associated key management infrastructure.

These security objectives are aligned with the high-level security objectives of FIPS 201-1. They protect both the integrity of the biometric authentication transaction and the privacy of the cardholder's biometric data, while avoiding the potential cost of reader authentication key management.

2. TEST PLAN

This test plan identifies the tasks required to design, develop and install the BMOC Performance Test Platform at the NIST test facility located in Gaithersburg, MD. The test plan also includes a necessary timeline to conduct BMOC performance tests as well as drafting a BMOC enabled PIV card edge protocol document.

Performing an external authentication with a smart card for physical access typically requires usage of the smart card's contactless interface. To better understand the feasibility of using a smart card for this purpose, timing metrics are required. The tests conducted in this report summarize the performance of several smart card readers with certified Personal Identity Verification cards. The performance of both the contact and contactless smart card interfaces are measured and compared.

Milestones:

4/30/07	Draft the BMOC Test Approach
5/1/07	Install BMOC issuance platform and Delivery of BMOC test cards
5/10/07	Personalize BMOC test card
5/16/07	Complete development of BMOC performance test platform
5/23/07	Collect initial performance measures of BMOC
5/24/07	NIST BMOC Workshop

3. TEST APPROACH

Our conceptual design is based on two observations. First, the PIV System trust model is founded on PKI, and by design, a PIV Card can authenticate itself to another system element using a private key and certificate stored on the card. Logically, this allows encrypted messages to be sent to the card, and signed messages to be returned from the card (thus satisfying SO1 and SO4). Second, if a biometric match operation is performed on the PIV Card using Match On Card (MOC) technology, there is no need to release biometric data from the PIV Card to any other system component (thus satisfying SO3).

In outline, the approach we propose works as follows. The cardholder presents their card to a contactless biometric reader, and presents their finger to the biometric scanner. The scanner obtains a fingerprint image which is transformed into the sample template, encrypted, and transmitted via contactless into the PIV Card. The PIV Card decrypts the template, matches the sample template against the reference template stored on the PIV Card, and returns the signed “Yes” or “No” result to the smart card reader.

An example of an abstract protocol sequence is included next. While we expect that devices under test will generally implement the abstract protocol, they may depart in detail. NIST will construct the test fixture (reader-side implementation) and must therefore have an complete specification of the implemented protocol. This specification will also be used to analyze the implemented protocol against the security objectives. The abstract protocol sequence is subject to change in the course of testing and in future standards development.

1. The cardholder presents their finger to the fingerprint scanner. The fingerprint scanner scans the finger, and generates the sample template from the image. Alternatively for test purposes, the finger print template is retrieved from a file. [1]

[1] Steps (1) can be performed at any time prior to Step (8), when the result of Step (1) is first used.

2. The cardholder presents their PIV Card to the contactless smart card reader.
3. The host system selects the Biometric MOC application on the card.

```
APDU-00 A4 04 00 10 A0 00 00 00 77 01 00 00 06 10 00 FF 00 00 00 25 00
```

4. The smart card reader performs Get Data to read the PKI certificate from the PIV Card, and validates the PKI certificate.

- GET DATA – Used with the BER-TLV tag for X.509 Certificate for Card Authentication to retrieve the certificate from a smart card.

```
APDU-00 CB 3F FF 05 5C 03 5F C4 10 00
```

- GET RESPONSE – Used to retrieve the response to the GET DATA APDU. Multiple GET RESPONSE APDUs may be required to retrieve the entire certificate data.

```
APDU-00 C0 00 00 00
```

5. The host system gets the nonce (a random card data) from the card.

- GET CHALLENGE – Used to retrieve a nonce that will be used for secure messaging.

```
APDU-00 84 00 00 00 18
```

- GET RESPONSE – Used to retrieve the response to the GET CHALLENGE APDU. The card responds with 8-bytes Rc(1) and 16 bytes Rc(2). Rc(1) is used to authenticate the host and Rc(2) is used to derive the session keys.

```
APDU-00 C0 00 00 00
```

6. The card authenticates to the host system, and the card and host system generate encryption and MAC session keys.

- GENERAL AUTHENTICATE – Used to communicate the session keys in an ciphered data block encrypted by the card public key.

```
APDU-00 86 06 00 80 data (1024 bit) 09
```

The encryption uses the following input data:
Random number for encryption session key (PSKenc)– 16 bytes
Random number for MAC session key (PSKmac) – 16 bytes
Rc(1) – 8 bytes padding received from GET CHALLENGE apdu

0x80 – 1 byte for tag padding
0x00 – 87 bytes fo zeros.

- GET RESPONSE – Used to retrieve the session ID and MAC.

```
APDU-00 C0 00 00 00
```

7. A secure session is established between the card and the host system. Both the card and the host system use the Rc(2) as a key to compute encryption session key and MAC session key. The algorithm is: SKmac = 3DES(PSKmac, Rc(2)) and SKenc = 3DES(PSKenc, Rc(2)).
8. The smart card reader encrypts the sample template using the session encryption key.
9. The host system send the template to the card for authentication

- VERIFY – Used to send ecrypted biometric template for authentication.

  ```
  APDU-00 20 00 02 length data 09
  ```

  The input data should be of the following format:
  0x7F 0x2E || length || 0x81 || length || encrypted biometric template (pad the tremplate with zero at the end to make it multiple of 8 bytes.

- GET RESPONSE – Used to retrieve the response to the VERIFY APDU. The reponse of 90 00 means the biometric template matched. The message also responds with 9 bytes of MAC for further verification by the host system.

```
APDU-00 C0 00 00 00
```

The test fixture will record the duration of each command-response transaction between the host and the card. A test record will therefore contain a complete log of all APDUs exchanged, and timings on each request-reponse pair individually. A trial will run tests repetitively to allow estimation of variance. Trials will be run with matching sample and reference templates, and with non-matching sample and reference templates, to highlight any differences in transaction time arising from the match result. If the reference template object contains multiple templates, trials will be designed to disclose the effects of multiple templates (e.g., separate trials matching first template vs. second template, and non-matching). The analysis of experimental data will offer conclusions on variance, break down communication and processing time per request-response cycle, document the amount of data transmitted (in both directions) during the protocol scenario, and estimate the command-response time per sub-activity (e.g., “read certificate”, “general authenticate”, “verify”).

The target transaction time for the secure BMOC technical feasibility study is performance of Steps 3 through 9 above in less than 2.5 seconds.